

Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Algoritma *Diversity* Untuk Keamanan Pesan

¹Aji Legawa, ²Sapri, ³Ockhy Jey Fhiter Wassalam

¹ Mahasiswa, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Alamat : Perum. Taman Kandis Raya Rt 20. Rw.01 Kel.Sumber Jaya Kec. Kamoung Melayu Kota Bengkulu,
email : ajilegawa55@gmail.com

^{2,3} Dosen Tetap, Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail: sapri@unived.ac.id, Ockhy@unived.ac.id

(Received: Juni 2026, Revised: Agustus 2026, Accepied: Oktober 2026)

Abstract-Advances in digital technology and the internet have necessitated information security systems that not only protect the content of messages but also conceal the existence of the messages themselves. Steganography offers an alternative solution by embedding secret messages into other media, such as digital images. This study aims to design and develop a steganography application for digital images using the Diversity algorithm to enhance message security. The Diversity algorithm leverages color variations in images to embed message bits more randomly, making them difficult to detect. The research method employed is applied research with a system design and implementation approach. The Diversity algorithm is applied by utilizing color variations in digital images to embed message bits, resulting in a more random embedding pattern that is difficult to analyze. The research results show that the system is capable of performing the text message embedding and extraction processes effectively without damaging the original information, and the visual quality of the steganography cally processed image is maintained. Thus, this application is effective as a means of securing messages based on digital images.

Keywords: Steganography, Digital Images, Diversity Algorithm, Message Security,

Intisari-Perkembangan teknologi digital dan internet menuntut adanya sistem pengamanan informasi yang tidak hanya melindungi isi pesan, tetapi juga menyembunyikan keberadaan pesan itu sendiri. Steganografi menjadi solusi alternatif dengan menyisipkan pesan rahasia ke dalam media lain, salah satunya citra digital. Penelitian ini bertujuan untuk merancang dan membangun aplikasi steganografi pada citra digital menggunakan algoritma Diversity guna meningkatkan keamanan pesan. Algoritma Diversity memanfaatkan perbedaan warna pada citra untuk menyisipkan bit pesan secara lebih acak sehingga sulit terdeteksi. Metode penelitian yang digunakan adalah penelitian terapan (applied research) dengan pendekatan perancangan dan implementasi sistem. Algoritma Diversity diterapkan dengan memanfaatkan perbedaan warna pada citra digital untuk menyisipkan bit pesan, sehingga pola penyisipan menjadi lebih acak dan sulit dianalisis. Hasil penelitian menunjukkan bahwa sistem mampu melakukan proses penyisipan dan ekstraksi pesan teks dengan baik tanpa merusak informasi asli, serta kualitas citra hasil steganografi tetap terjaga secara visual. Dengan demikian, aplikasi ini efektif sebagai sarana pengamanan pesan berbasis citra digital.

Kata Kunci Steganografi, Citra Digital, Algoritma Diversity, Keamanan Pesan,

I.PENDAHULUAN

Perkembangan teknologi digital dan penetrasi internet yang masif telah menjadikan pertukaran

informasi melalui media digital sebagai sebuah keniscayaan. Aktivitas berbagi data sensitif, seperti rahasia dokumen pribadi, atau komunikasi strategis, memerlukan jaminan kerahasiaan (*confidentiality*) dan integritas yang tinggi. Kriptografi, sebagai ilmu untuk mengacak data, telah menjadi solusi utama. Namun, data terenkripsi (ciphertext) yang dikirimkan justru dapat menarik perhatian pihak ketiga yang tidak berkepentingan, memicu upaya cracking yang lebih agresif (Kadarisman et al., 2021). Oleh karena itu, diperlukan pendekatan keamanan yang tidak hanya melindungi isi pesan tetapi juga menyembunyikan keberadaan (*existence*) pesan itu sendiri. Steganografi, seni dan ilmu menyembunyikan pesan rahasia ke dalam media penampung (cover object) sehingga tidak menimbulkan kecurigaan, muncul sebagai solusi komplementer yang efektif. Citra digital merupakan media penampung yang paling populer dalam steganografi karena redundancy data yang tinggi dan sifat statistiknya yang kompleks, sehingga sulit dideteksi oleh indera manusia (Pratama et al., 2022). Steganografi merupakan seni atau praktik menyembunyikan pesan, citra, atau file kedalam pesan, citra atau file yang lain. Steganografi memiliki kelebihan tersendiri dibandingkan dengan kriptografi dimana pesan rahasia tidak menarik perhatian karena bersifat tersembunyi pada media lain. Dalam

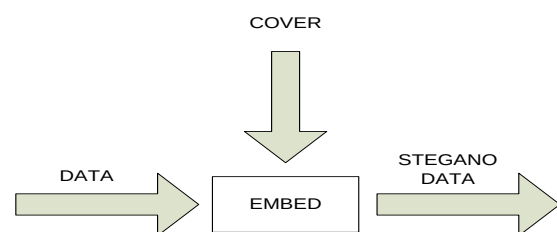
steganografi digital, komunikasi elektronik dapat mencakup steganografi coding dalam lapisan transport, seperti file dokumen, file gambar, program atau protokol. File media umumnya sangat ideal untuk transmisi steganografi karena ukurannya yang besar. Steganografi pada saat ini telah banyak diterapkan memanfaatkan citra digital. Berbagai teknik dan algoritma telah berkembang dan digunakan dalam implementasi steganografi pada citra digital. Salah satu metode yang cukup dikenal pada steganografi adalah metode *Diversity*. Metode *diversity* merupakan metode mengedepankan dan memaksimalkan perbedaan warna yang terdapat dalam citra digital. Pada citra 8-bit, jumlah warna terbatas, hanya 256 warna. Pengubahan format citra 8-bit menjadi 24 bit akan menghasilkan warna baru (yang semula tidak terdapat di dalam palet RGB). Penerapan metode *diversity* ini diyakini dapat meningkatkan keamanan (*security*) karena membuat pola penyisipan menjadi sangat tidak teratur dan sulit dimodelkan oleh alat stegoanalisis. Selain itu, pendekatan ini juga dapat dioptimalkan untuk mempertahankan kualitas citra (*imperceptibility*) dan meningkatkan kapasitas penyimpanan (Sari & Hidayat, 2023).

II. TINJAUAN USTAKA

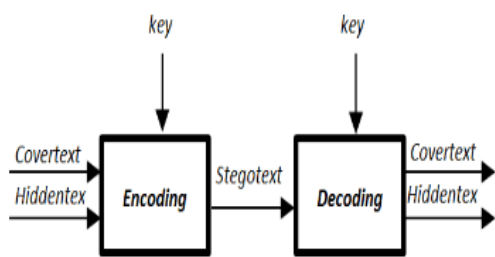
A. Pengertian Steganografi

Steganografi adalah salah satu alternatif solusi dalam mengamankan informasi yang bersifat penting dan pribadi. Istilah steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau menyembunyikan dan *graphein* yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama (Wibisono, Waluyo, & Ujianto, 2020). Steganografi

merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan atau informasi rahasia didalam informasi lainnya. Steganografi mempunyai sejarah yang hampir sama dengan kriptografi, keduanya banyak digunakan ketika zaman perang (Syahril & Jaya, 2019). Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia (Simbolon, 2021). Contoh singkat yang dapat dijelaskan adalah pengirim memilih gambar yang ingin dititipi informasi, kemudian mengatur setiap warna pixel ke-100 untuk menyesuaikan huruf dalam alphabet. Setiap perubahan yang terjadi diamati dan dicatat, perubahan yang begitu halus atau tanpa cacat dalam kondisi fisik gambar tersebut sehingga tidak ada pihak lain yang menyadarinya bahwa didalam gambar tersebut terdapat sebuah informasi yang bersifat rahasia jika pihak lain tidak benar-benar memperhatikannya menggunakan aplikasi untuk mendeteksi informasi tersembunyi dalam gambar digital. Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia (Lutfi & Rosihan, 2018).



Gambar 1 Proses Steganografi



Gambar2. Kerja Steganografi Secara Umum

Pada Gambar 2.2, dijelaskan bahwa penyisipan pesan kedalam *cover text* dinamakan *encoding*, sedangkan ekstraksi pesan *stego text* dinamakan *decoding*. Kedua proses ini memerlukan kunci rahasia (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Ada beberapa istilah penting dalam steganografi menurut (Wibisono, Waluyo, & Ujianto, 2020) antara lain :

1. *Cover-Object*

Objek asli yang digunakan untuk menyembunyikan informasi

2. *Message*

Informasi atau pesan aktual yang disembunyikan. Pesan dapat berupa teks atau gambar.

3. *Stego-Object*

Menyisipkan pesan atau informasi rahasia ke dalam *cover object*

4. *Stego-Key*

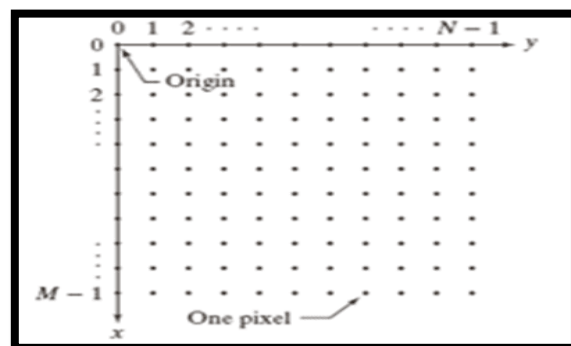
Kunci yang digunakan untuk menyisipkan atau mengekstraksi pesan dari *cover object* dan *stego-object*, kunci dapat berupa huruf, angka ataupun simbol

a. Citra Digital

i. Pengertian Citra Digital

Citra atau gambar dapat didefinisikan sebagai fungsi dua dimensi $f(x,y)$, dimana x dan y adalah kordinat bidang datar; dan harga fungsi f di setiap pasangan kordinat (x,y) disebut intensitas atau level keabuan (greylevel) dari gambar di titik itu. Apabila nilai x,y dan f secara keseluruhan berhingga (finite) dan

bernilai diskrit maka dapat dikatakan bahwa citra tersebut adalah citra digital (Jumadi, dkk 2020). Pengolahan citra merupakan cabang ilmu dalam Artificial Intelegence yang menggunakan objek citra dalam bentuk digital untuk penyelesaian kasusnya. Metode dalam citra dapat digunakan baik perhitungan matematis pada objek secara piksel ataupun geometris. Masing-masing objek citra memiliki nilai perbedaan yang dapat diperhitungkan secara matematis, sehingga menunjukkan ciri yang berbeda antara objek satu dengan yang lain. Penciri dari perbedaan setiap objek dapat ditentukan dari warna, tekstur, ataupun bentuk (Jumadi, dkk, 2021) Citra digital dibentuk oleh kumpulan titik yang dinamakan piksel (pixel atau “picture element”). Setiap piksel digambarkan sebagai satu kotak kecil. Setiap piksel mempunyai koordinat posisi.



Gambar 3. Ilustrasi Citra Digital

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, di mana perpotongan antara kolom dan baris disebut piksel, yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah $f(x,y)$, yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah citra digital dapat ditulis dalam bentuk matriks berikut:

$$f(x,y) = \begin{bmatrix} f(0,0) & \cdots & f(0,M-1) \\ \vdots & \ddots & \vdots \\ f(N-1,0) & \cdots & f(N-1,M-1) \end{bmatrix}$$

Berdasarkan gambaran tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas $f(x,y)$, di mana harga x (baris) dan y (kolom) merupakan koordinat posisi dan $f(x,y)$ adalah nilai fungsi pada setiap titik (x,y) yang menyatakan besar intensitas citra atau tingkat keabuan atau warna dari piksel di titik tersebut. Pada proses digitalisasi (sampling dan kuantisasi) diperoleh besar baris M dan kolom N hingga citra membentuk matriks $M \times N$ dan jumlah tingkat keabuan piksel. Pada kebanyakan kasus, terutama untuk keperluan penampilan secara visual, nilai data visual tersebut merepresentasikan warna dari citra yang diolah, dengan demikian format data citra digital berhubungan erat dengan warna

III. METODOLOGI PENELITIAN

A. Metode Penelitian

Dalam melakukan penelitian ini, penulis menggunakan metode terapan (*applied research*). Penelitian terapan atau *applied research* dilakukan berkenaan dengan kenyataan-kenyataan praktis, penerapan, dan pengembangan ilmu pengetahuan yang dihasilkan oleh penelitian dasar dalam kehidupan nyata. Penelitian terapan berfungsi untuk mencari solusi tentang masalah-masalah tertentu. Tujuan utama penelitian terapan adalah pemecahan masalah sehingga hasil penelitian dapat dimanfaatkan untuk kepentingan manusia baik secara individu atau kelompok maupun untuk keperluan industri atau politik dan bukan untuk wawasan keilmuan semata. Dalam melaksanakan penelitian terapan ini terdapat 5 (lima) langkah, diantaranya :

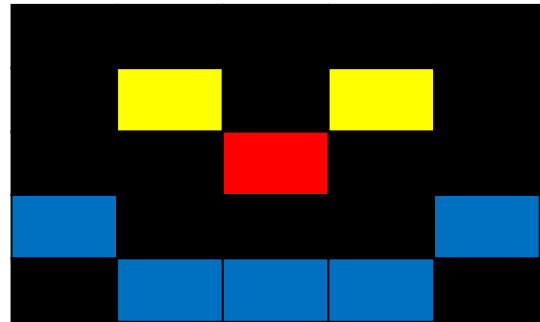
- Melakukan sesuatu yang sedang diperlukan, dipelajari, diukur, dan diperiksa kelemahannya.
- Mencari satu dari kelemahan-kelemahan yang diperoleh dipilih untuk penelitian.
- Mencari dan memberikan solusi dalam melakukan pemecahan masalah

- Kemudian dilakukan modifikasi sehingga penyelesaian dapat dilakukan untuk diterapkan.
- Pemecahan dipertahankan dan menempatkannya dalam suatu kesatuan sehingga jadi bagian permanen dalam satu sistem.

A. Analisa Metode Steganografi Diversity Pada Citra Digital

Steganografi menggunakan algoritma diversity pada konsepnya adalah menyisipkan bit karakter pada senarai warna terpilih yang memiliki jarak warna yang berjauhan. Adapun langkah – langkah proses steganografi pada metode diversity adalah sebagai berikut :

- Menyiapkan citra digital yang akan disisipkan:



- Menyiapkan pesan yang akan disembunyikan : UNHAR dan mengkonversi karakter kedalam bit biner.

U = 0101 0101, N = 0100 1110, H = 0100 1000, A = 0100 0001, R = 0101 0010

Deretan bit : 0101010101001110010010000100000101010010

- Menyusun histogram warna dari citra yang digunakan.

No	Warna	Frekuensi	Posisi Piksel
1	0,0,0 (Hitam)	17	P1, P2, P3, P4, P5, P6, P8, P10, P11, P12, P14, P15, P17, P18, P19, P21, P25
2	255, 255, 0 (Kuning)	2	P7, P9
3	255,0,0 (Merah)	1	P13
4	0,0,255 (Biru)	5	P16, P20, P22, P23, P24

4. Mengambil piksel dengan frekuensi terbesar untuk masuk kedalam senarai warna awal.

Piksel terpilih adalah piksel hitam (0,0,0) dengan frekuensi 17 piksel.

5. Berikutnya adalah menghitung jarak warna terjauh dengan warna acuan yang sudah berada didalam senarai warna awal.

$$D(Kuning, Hitam)$$

$$= \sqrt{(255 - 0)^2 + (255 - 0)^2 + (0 - 0)^2}$$

$$= 360.62$$

$$D(Merah, Hitam)$$

$$= \sqrt{(255 - 0)^2 + (0 - 0)^2 + (0 - 0)^2} = 255$$

$$D(Biru, Hitam)$$

$$= \sqrt{(255 - 0)^2 + (255 - 0)^2 + (0 - 0)^2} = 255$$

6. Dari perhitungan jarak diatas diperoleh warna terjauh dari warna senarai awal adalah warna kuning sehingga warna tersebut akan dimasukkan kedalam senarai warna dimana senarai warna menjadi :

Senarai Warna = {Hitam, Kuning}

7. Proses dilanjutkan dengan mengulangi langkah 5 namun menggunakan dua acuan warna yaitu hitam dan kuning.

$$D(Merah, Hitam)$$

$$= \sqrt{(255 - 0)^2 + (0 - 0)^2 + (0 - 0)^2} = 255$$

$$D(Merah, Kuning)$$

$$= \sqrt{(255 - 255)^2 + (0 - 255)^2 + (0 - 0)^2}$$

$$= 255$$

$$D(Biru, Hitam)$$

$$= \sqrt{(0 - 0)^2 + (0 - 0)^2 + (255 - 0)^2} = 255$$

$$D(Biru, Kuning)$$

$$= \sqrt{(0 - 255)^2 + (0 - 255)^2 + (255 - 0)^2}$$

$$= 441.67$$

8. Dari perhitungan jarak diatas maka dapat diperoleh Biru adalah warna terjauh dari senarai

warna saat ini sehingga Biru akan dimasukkan kedalam senarai warna.

Senarai Warna = {Hitam, Kuning, Biru}

9. Dikarenakan warna yang tersisa adalah Merah maka Merah juga akan dimasukkan kedalam senarai warna pada posisi terakhir.

Senarai Warna = {Hitam, Kuning, Biru, Merah}

10. Proses penyisipan dilakukan pada piksel dari senarai warna yang pertama dan diteruskan pada senarai warna berikutnya jika senarai pertama tidak mencukupi.

11. Pada senarai warna diperoleh warna pertama adalah Hitam yang mana terdiri dari 17 buah piksel yang akan digunakan sebagai piksel penampung sebagai berikut.

P1 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000
disisipkan dengan tiga buah bit awal dari pesan yaitu 010 pada posisi LSB sehingga warna baru dari P1 adalah :

$$P1 = 0000 0000, 0000 0001, 0000 0000 = 0,1,0$$

Deretan bit sisa :

$$1010101001110010010000100000101010010$$

P2 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000
disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 101 pada posisi LSB sehingga warna baru dari P2 adalah :

$$P2 = 0000 0001, 0000 0000, 0000 0001 = 1,0,1$$

Deretan bit sisa :

$$0101001110010010000100000101010010$$

P3 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000
disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 010 pada posisi LSB sehingga warna baru dari P3 adalah :

$$P3 = 0000 0000, 0000 0001, 0000 0000 = 0,1,0$$

Deretan bit sisa :

$$1001110010010000100000101010010$$

P4 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000
disisipkan dengan tiga buah bit berikutnya dari

pesan yaitu 100 pada posisi LSB sehingga warna baru dari P4 adalah :

$$P4 = 0000\ 000\mathbf{1}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0} = 1,0,0$$

Deretan bit sisa : 1110010010000100000101010010

P5 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 111 pada posisi LSB sehingga warna baru dari P5 adalah :

$$P5 = 0000\ 000\mathbf{1}, 0000\ 000\mathbf{1}, 0000\ 000\mathbf{1} = 1,1,1$$

Deretan bit sisa : 0010010000100000101010010

P6 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 001 pada posisi LSB sehingga warna baru dari P6 adalah :

$$P6 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1} = 0,0,1$$

Deretan bit sisa : 0010000100000101010010

P8 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 001 pada posisi LSB sehingga warna baru dari P8 adalah :

$$P8 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1} = 0,0,1$$

Deretan bit sisa : 0000100000101010010

P10 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 000 pada posisi LSB sehingga warna baru dari P10 adalah :

$$P10 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0} = 0,0,0$$

Deretan bit sisa : 0100000101010010

P11 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 010 pada posisi LSB sehingga warna baru dari P11 adalah

$$P11 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1}, 0000\ 000\mathbf{0} = 0,1,0$$

Deretan bit sisa : 0000101010010

P12 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 000 pada posisi LSB sehingga warna baru dari P12 adalah

$$P12 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0} = 0,0,0$$

Deretan bit sisa : 0101010010

P14 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 010 pada posisi LSB sehingga warna baru dari P14 adalah

$$P14 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1}, 0000\ 000\mathbf{0} = 0,1,0$$

Deretan bit sisa : 1010010

P15 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 010 pada posisi LSB sehingga warna baru dari P15 adalah

$$P15 = 0000\ 000\mathbf{1}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1} = 1,0,1$$

Deretan bit sisa : 0010

P17 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 001 pada posisi LSB sehingga warna baru dari P17 adalah

$$P17 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{1} = 0,0,1$$

Deretan bit sisa : 0

P18 = 0,0,0 = 0000 0000, 0000 0000, 0000 0000 disisipkan dengan tiga buah bit berikutnya dari pesan yaitu 000 pada posisi LSB sehingga warna baru dari P18 adalah

$$P18 = 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0}, 0000\ 000\mathbf{0} = 0,0,0$$

12. Setelah proses penyisipan selesai tahap berikutnya adalah menulis kembali nilai warna hasil penyisipan kedalam citra.

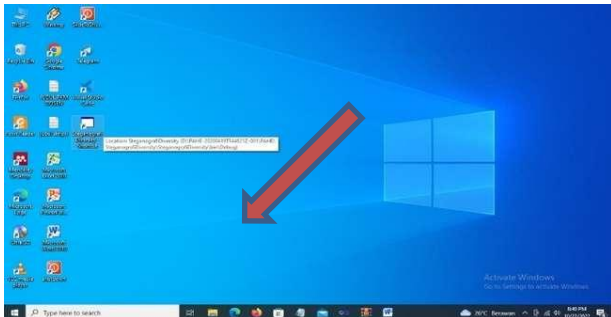
No	Piksel	Warna Lama	Warna Baru
1	P1	0,0,0	0,1,0
2	P2	0,0,0	1,0,1
3	P3	0,0,0	0,1,0
4	P4	0,0,0	1,0,0
5	P5	0,0,0	1,1,1
6	P6	0,0,0	0,0,1
7	P8	0,0,0	0,0,1
8	P10	0,0,0	0,0,0
9	P11	0,0,0	0,1,0

No	Piksel	Warna Lama	Warna Baru
10	P12	0,0,0	0,0,0
11	P14	0,0,0	0,1,0
12	P15	0,0,0	1,0,1
13	P17	0,0,0	0,0,1

IV. HASIL DAN PEMBAHASAN

A. Hasil Aplikasi

Aplikasi penerapan metode *Steganografi Diversity* dibangun sesuai dengan analisa dan perancangan seperti yang telah dijabarkan pada bab sebelumnya yaitu bab metodologi penelitian, maka pada bagian ini akan dipaparkan hasil dari aplikasi yang dibangun menggunakan perancangan yang telah dilakukan pada bab sebelumnya. Pada bab ini pembahasan akan dilakukan terhadap hasil dari sistem yang dibangun, fungsional sistem dan analisis terhadap kinerja sistem berdasarkan hasil *output* yang dihasilkan oleh sistem.



Gambar 4. Shortcut Aplikasi *Steganografi Diversity* di Desktop

Implementasi dan Pembahasan

Implementasi sistem merupakan tahap bagaimana sistem untuk dijalankan berdasarkan desain yang telah dibuat dan dirancang pada tahap sebelumnya kemudian dimasukkan ke bahasa pemrograman yang digunakan. Implementasi ini menggunakan bahasa pemrograman VB.NET. Penerapan metode steganografi diversity pada sistem yang dibangun yaitu dalam proses penyisipan data teks pada data citra digital dengan ekstensi .bmp.



Gambar 5. Citra bmp Uji Coba

Citra digital diatas akan dijadikan sebagai citra penampung yang akan bekerja sebagai penampung informasi rahasia yang akan melewati proses steganografi. Selanjutnya setelah menentukan citra uji atau citra penampung, penulis akan membuka aplikasi steganografi diversity yang telah dibuat oleh penulis. Sebelum hal ini dilakukan penulis akan terlebih dahulu menjabarkan halaman-halaman yang ada beserta dengan fungsi dari masing-masing halaman yang ada pada aplikasi.

1. Form Menu Utama

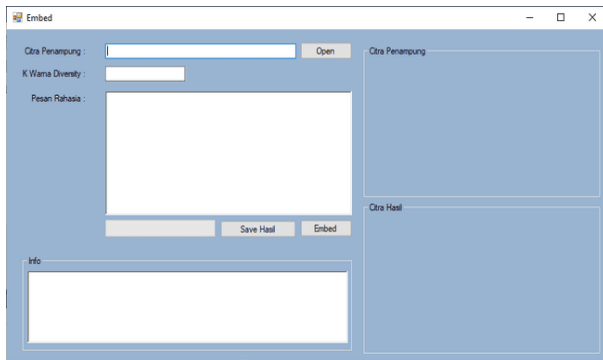
Form ini merupakan yang pertama muncul ketika membuka sistem. Pada form ini akan diminta user untuk memilih antara proses *embed* data, *extract* data, dan keluar



Gambar 6. Form Menu Utama

2. Form Embed

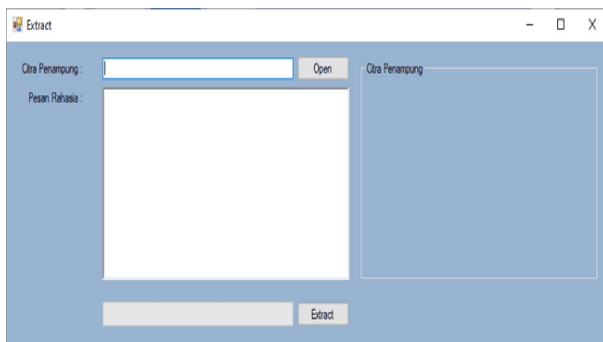
Seperti yang terlihat pada gambar yang merupakan form Utama. Setelah menekan tombol *embed*, maka sistem akan menampilkan halaman seperti berikut :



Gambar 7. Form Embed

3. Form Extract

Pada *form extract* ini akan ditampilkan halaman yang dikhususkan untuk proses ekstraksi data dari citra yang sudah melewati proses steganografi



Gambar 8. Form Extract

4.1 Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui bagaimana jalannya kerja sistem dalam melakukan steganografi data citra digital .bmp atau embed dan kemudian mengembalikannya ke kondisi semula dengan proses extract atau mengambil kembali informasi dari citra digital

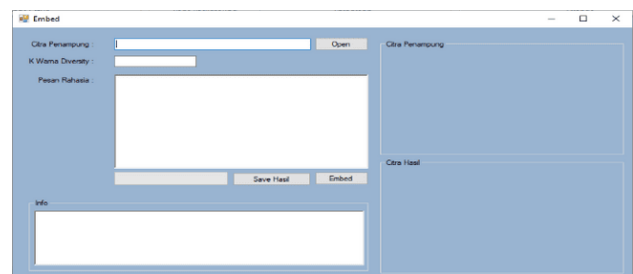
Pengujian Embed Pesan Pada Citra Digital

Pada bagian ini, akan dilakukan pengujian fungsi algoritma yang digunakan dalam sistem, yaitu *Steganografi Diversity*. Pengujian yang dilakukan menggunakan data citra digital dengan nama laptop.bmp dengan besar data 79.1 KB



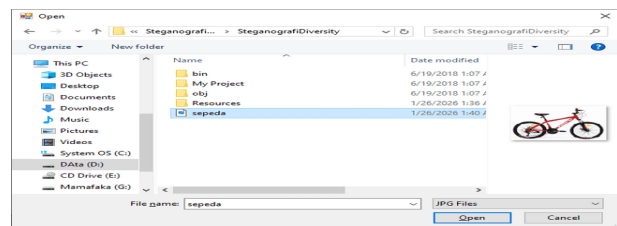
Gambar 9. Citra Test

Selanjutnya pengguna akan membuka aplikasi dan memilih tombol embed. Setelah menekan tombol embed selanjutnya pengguna akan dipindahkan pada halaman khusus untuk proses steganografi. Berikut tampilan halaman kompresi pada sistem



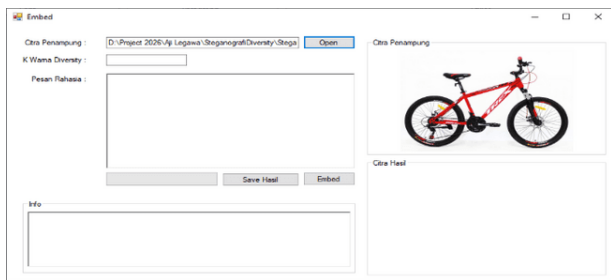
Gambar 10. Halaman Embed

Selanjutnya pengguna akan menginputkan gambar pada sistem. Gambar yang akan diinputkan adalah gambar yang sebelumnya sudah diperkenalkan yaitu Laptop.bmp dengan besar data 79.1 KB. Berikut tampilan sistem pada saat pemilihan data citra digital yang akan diinput kedalam sistem :



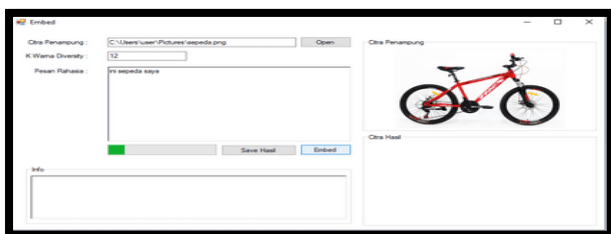
Gambar 11. Pemilihan Citra Digital Steganografi Diversity

Setelah proses input selesai halaman embed akan menampilkan data seperti berikut:



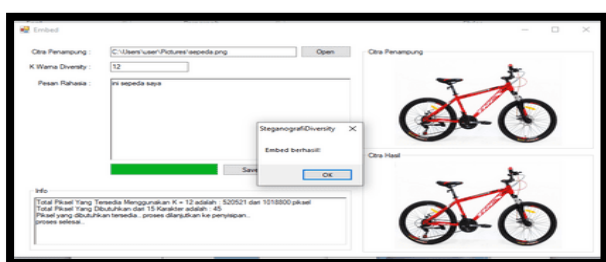
Gambar 12. Input Citra Kedalam Sistem

Setelah data siap diinputkan kedalam sistem langkah selanjutnya adalah memasukkan jumlah K sebagai penentu warna diversity yang kemudian akan dilanjutkan dengan memasukkan pesan rahasia yang ingin di masukkan pada citra. Pada pengujian ini penulis akan memasukkan pesan sebagai berikut “Universitas Dehasen Jaya Selalu” dengan panjang K=12. Setelah itu, penulis akan menekan tombol “Embed” yang akan menjalankan sistem secara otomatis dan akan meng-embed data teks pada citra yang dipilih sistem akan menjalankan proses steganografi secara otomatis seperti yang tampak pada gambar berikut;



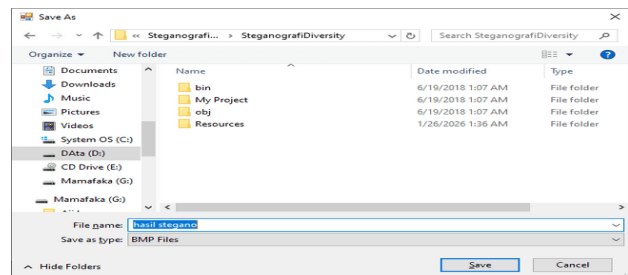
Gambar 13. Proses Embed Pesan Pada Citra

Selama proses kompresi dilakukan, sistem pertama kali akan membaca data piksel dan kemudian memetakannya dan mengubahnya sesuai dengan kamus data dari algoritma. Setelah beberapa waktu, proses embed pun selesai dilaksanakan, hal ini ditandai dengan munculnya jendela yang menyatakan proses embed berhasil



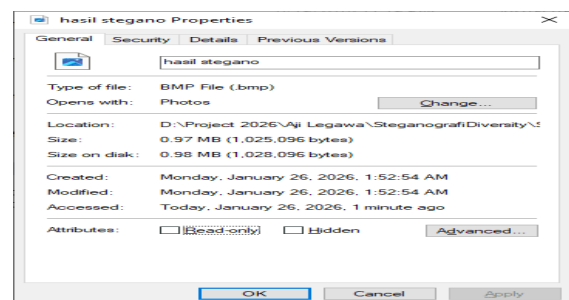
Gambar 14. Hasil Steganografi Diversity

Setelah proses embed data teks berhasil dilakukan langkah selanjutnya adalah menyimpan citra yang sudah melewati proses steganografi untuk nantinya akan dilakukan pengujian extract data dari citra stegano



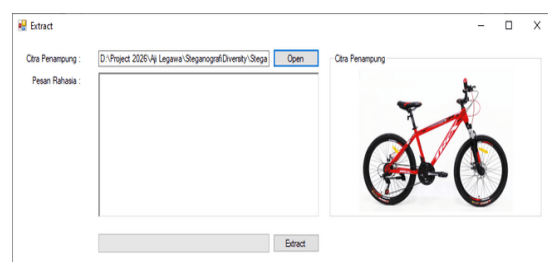
Gambar 15. Penyimpanan Hasil Steganografi

Setelah disimpan, file akan mengalami perubahan yang signifikan yang diakibatkan oleh perubahan ekstensi data dan juga dikarenakan adanya tambahan data pada piksel yang ada didalam citra



Gambar 16. Data Hasil Steganografi

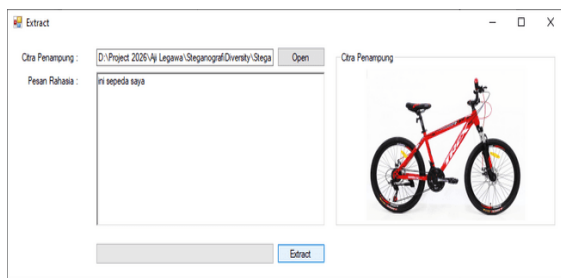
Selanjutnya dengan menggunakan data citra digital yang sama atau hasil steganografi, penulis akan melanjutkan penulis akan melanjutkan pengujian dengan melakukan proses ekstraksi data dari citra steganografi. Proses ekstraksi dapat dilihat seperti yang tampak pada gambar berikut ini.



Gambar 17. Ekstraksi Data Dari Citra Stegano

Setelah proses pemilihan gambar stegano selesai selanjutnya penulis akan menekan tombol extract

yang ada didalam sistem seperti yang tampak pada gambar dibawah ini.



Gambar 18. Proses Extract Selesai

Setelah proses extract selesai dapat dilihat bahwa data atau teks rahasia yang sebelumnya kita masukkan kedalam citra dapat diextract dengan baik dan menghasilkan informasi yang sama tanpa mengurangi nilai asli dari informasi itu sendiri.

Berdasarkan hasil pengujian yang dilakukan oleh penulis dalam proses embed dan extract data pada citra digital, dapat diambil kesimpulan bahwa sistem telah menerima implementasi algoritma diversity dengan baik dan mampu melaksanakan proses steganografi dengan baik dan sesuai dengan algoritma yang diterapkan

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat diambil beberapa kesimpulan sebagai berikut:

1. Algoritma Diversity berhasil diterapkan pada sistem steganografi citra digital dengan memanfaatkan perbedaan warna sebagai dasar penyisipan pesan, sehingga pola penyisipan menjadi lebih acak dan sulit dianalisis secara visual
2. Aplikasi steganografi yang dibangun menggunakan Visual Basic .Net 2010 mampu melakukan proses penyisipan dan ekstraksi pesan teks dengan baik pada citra digital tanpa menghilangkan informasi asli pesan

3. Kualitas citra setelah proses steganografi tetap terjaga dan secara visual tidak menimbulkan perbedaan yang signifikan dibandingkan citra asli, sehingga memenuhi kriteria imperceptibility dalam steganografi.

4. Hasil pengujian menunjukkan bahwa sistem berjalan sesuai dengan perancangan dan algoritma yang digunakan mampu meningkatkan keamanan pesan pada media citra digital

B. Saran

Berdasarkan hasil penelitian ini, beberapa saran yang dapat diberikan untuk pengembangan selanjutnya adalah sebagai berikut :

1. Penelitian selanjutnya dapat mengembangkan sistem dengan menambahkan kombinasi metode kriptografi sebelum proses steganografi untuk meningkatkan tingkat keamanan pesan.
2. Aplikasi dapat dikembangkan menggunakan bahasa pemrograman atau platform yang lebih modern agar kompatibel dengan berbagai sistem operasi terbaru
3. Perlu dilakukan analisis kuantitatif lebih lanjut, seperti pengukuran PSNR atau MSE, untuk menilai kualitas citra hasil steganografi secara objektif

DAFTAR PUSTAKA

- [1] Alfina, O., & Harahap, F. (2019). Pemodelan UML Sistem Pendukung Keputusan Dalam Penentuan Kelas Siswa Siswa Tunagrahita. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi*, 143-150.
- [2] Ayumida, S., Azis, M. S., & Fiano, Z. G. (2020). Implementasi Program Administrasi Pembayaran Berbasis Dekstop (Studi Kasus: SMA NEGERI 1 CIKAMPEK). *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, 72-83.
- [3] Gunawan, I., & Sumarno. (2018). Penggunaan Algoritma Kriptografi Steganografi Least Significant

- Bit Untuk Pengamanan Pesan Teks dan Data Video. *J-Sakti (Jurnal Sains Komputer dan Informatika)*, 57-65.
- [4] Jumadi, J., Akbar, A. a., & Septiawan, S. E. (2020). Implementasi Metode Template Matching Untuk Klasifikasi Citra Anggrek Pensil Bengkulu. *Konferensi Nasional Ilmu Komputer (KONIK). I. Makasar: KONIK 2020*.
- [5] Jumadi, J., Yupianti, & Sartika, D. (2021). Pengolahan Citra Digital Untuk Identifikasi Objek Menggunakan Metode Hierarchical Agglomerative Clustering. *JST (Jurnal Sains dan Teknologi)*, 148-156
- [6] Limantoro, R. R., & Kristiadi, D. P. (2021). Pengembangan Sistem Informasi Pendataan Green Folder Menggunakan Metode Berorientasi Objek Dan UML Berbasis Web Pada TKHarvest Christian School. *JURNAL SISTEM INFORMASI DAN TEKNOLOG (SINTEK)*, 7-14.
- [7] Lutfi, S., & Rosihan. (2018). Perbandingan Metode Steganografi LSB (Least Significant Bit) Dan MSB (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra DIGITAL. *JIKO (Jurnal Informatika dan Komputer)*, 34-42.
- [8] Muafi, Wijaya, A., & Aziz, V. A. (2020). Sistem Pakar Mendiagnosa Penyakit Mata Pada Anusia Menggunakan Metode Forward Chaining. *Jurnal Komputasi dan Teknologi Informasi*, 43-49.
- [9] Sutrisno, J., & Karnadi, V. (2021). Aplikasi Pendukung Pembelajaran Bahasa Inggris Menggunakan Media Lagu Berbasis Android. *JURNAL COMASIE*, 31-41.
- [10] Syahril, M., & Jaya, H. (2019). Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4. *Seminar Nasional Sains & Teknologi Informasi (SENSASI)*, 505-509.
- [11] Wibisono, G., Waluyo, T., & Ujianto, E. (2020). Kajian Metode Metode Steganografi Pada Domain SpasiaL. *JTIK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, 251-256.
- [12] Yesputra, R. (2019). *Belajar visual basic. Netdengan visual studio 2010*. Medan: Royal Asahan Press.